PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	)
	)
Blamires et al.	) Group Art Unit: 2134
	)
Application No. 10/620,364	) Examiner: Simitoski, Michael J.
	)
Filed: 07/17/2003	) Docket No. NAI1P492/03.028.01
	)
For: MALWARE SCANNING USING A BOOT WITH A NON-INSTALLED OPERATING SYSTEM AND DOWNLOAD OF MALWARE DETECTION FILES	) Date: 04/10/2008

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 1.193)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer on 03/05/2008.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue # 1:

Group #1: Claims 1-3, 7-11, 15-19, 23-25 and 28

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the obviousness of combining the Reinert and Yadav references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert [with Yadav] to connect to the remote computer via a secure connection." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Reinert and Yadav references, especially in view of the vast evidence to the contrary.

Specifically, the Reinert reference teaches that "the present invention discloses a method and apparatus for providing up-to-date virus scanning of a local computer by a remote computer comprising those situations where the normal operating system of the local computer is not operable" (Col. 3, lines 44-48 - emphasis added). On the other hand, the Yadav reference teaches "[n]etwork intrusion detection [that] accurately identifies and takes into consideration currently running network applications by examining machine instructions embodying those applications" (Abstract, lines 1-4 - emphasis added).

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not

sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

Combining a method where the normal operating system is not operable, as in Reinert, with an intrusion detection system that takes into consideration currently running network applications, as in Yadav, would require an impermissible change in the principle of operation of Reinert, contrary to *In re Ratti*. Thus, the Examiner's proposed combination is inappropriate. To this end, the first element of the *prima facie* case of obviousness has not been met.

In the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "col. 7, lines 49-51 uses the language 'even if' to describe the event where the local operating system is not operable and as such it is not a requirement of Reinert that the local operating system be nonfunctional," and that therefore "[t]he invention disclosed also works in those situations where the local operating system is not operational."

Appellant respectfully disagrees. The excerpt from Reinert referenced by the Examiner simply discloses that "[o]ne advantage of the preferred embodiment in accordance with the present invention is that the local computer 42 may boot up even if its normal operating system program has been rendered inoperable by a virus or other catastrophic event" (Col. 7, lines 47-51). However, appellant again points out that Reinert explicitly discloses that "[to] overcome the limitations in the prior art...the present invention discloses a method and apparatus for providing up-to-date virus scanning of a local computer by a remote computer comprising those situations where the normal operating system of the local computer is not operable" (Col. 3, lines 41-48 - emphasis added). Thus, Reinert expressly relates to providing up-to-date virus scanning of a local computer only in a situation where a normal operating system of the local computer is not operable, contrary to the Examiner's suggestion otherwise.

Also in the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "Yadav is cited for teaching a benefit of creating a secure connection (as opposed to a non-secure connection), such as a VPN or SSL connection, when updating signatures/definitions for an intrusion detection system." The Examiner has also argued that "[a]s Reinert's invention comprises a

working virus scanning program that contacts a remote server (described at least at Reinert, col. 7, lines 49-67), Reinert's invention would equally benefit from the increase security and integrity of a secure connection between the local computer and the remote server."

Appellant respectfully disagrees. For example, appellant respectfully asserts that Reinert does not disclose "a working virus scanning program that contacts a remote server," as suggested by the Examiner. Specifically, Reinert only teaches that "[t]he local user may execute a virus scanning program and if one or more viruses are detected on the local computer 42, the user may connect to the remote computer 54" (Col. 7, lines 62-65 - emphasis added), where "a communications program is invoked by the local user to establish a communications connection between the local computer 42 and the remote computer 54" (Col. 7, line 66-Col. 8, line 1). Accordingly, appellant again respectfully asserts that the Examiner's proposed combination is inappropriate, and that therefore the first element of the *prima facie* case of obviousness has not been met.

More importantly, appellant also respectfully asserts that the third element of the *prima facie* case of obviousness has not been met by the prior art excerpts relied on by the Examiner. For example, with respect to the independent claims, the Examiner has relied on Col. 7, lines 4-5 and lines 65-67 from Reinert; paragraphs 0042-0044 from Yadav; pages 320-323, and the "private network" in Fig. 10.1(a) from Stallings to make a prior art showing of appellant's claimed technique "wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "[i]f any viruses are detected, the user may then connect to the remote computer utilizing the communications program" (Col. 7, lines 4-5), and that "[i]f the local user desires to connect with the remote computer 54, a communications program is invoked by the local user to establish a communications connection" (Col. 7, lines 65-67 – emphasis added). Additionally, the excerpts from Yadav merely teach that "the SOC 270 and the NIDS may communicate over a virtual private network (VPN) 284, with its own encryption and security features, or use Secure

Sockets Layer (SSL) to create a secure connection" (Paragraph 0044). Furthermore, the excerpts cited from Stallings only generally teach "FIREWALL DESIGN PRINCIPLES" (see page 320), which includes general information on "Firewall Characteristics" (see page 321) and "Types of Firewalls" (see page 322). Moreover, Fig. 10.1(a) from Stallings merely illustrates a "Packet-filtering router" between the "Internet" and the "Private network."

However, disclosing that a user may connect to a remote computer utilizing a communications program (see Reinert), utilizing a VPN or a SSL to create a secure connection (see Yadav), along with a general firewall description (see Stallings), fails to specifically teach that "network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (emphasis added), as claimed by appellant. Appellant respectfully asserts that only appellant teaches and claims the loading of network support code from removable physical media which specifically enables the secure network connection via the firewall, in the context claimed.

In addition, the Examiner has specifically argued that "[i]n light of [appellant's previous] amendments, the Stallings reference is submitted," and that "[a]s herein modified, the code [of Reinert] is also used to establish the secure connection via said firewall, as the packets must traverse the firewall for reception at the remote computer" (see page 5 of the Office Action dated 05/15/2007). Appellant respectfully disagrees and asserts that even in view of the improper combination of the Reinert, Yadav, and Stallings references, the proposed combination fails to teach or suggest that "said network support code is used to **enable** said computer to establish said secure network connection **via said firewall** computer to said remote computer" (emphasis added), in the context claimed by appellant, for at least the reasons noted above.

In the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "Reinert discloses a system that utilizes a bootable media to boot a computer and execute a virus scanning application and to further execute a communications program (the claimed support code) to contact a remote server for, among other things, downloading updates to virus definition files (see col. 7, lines 49-67and specifically, col. 7, line 65 - col. 8, line 1 & col. 8, lines 23- 25)." The Examiner has additionally argued that "[a] firewall is an application/device that protects a local system or

network from network-based security threats (Stallings, p. 320, [paragraph] 1) where only authorized traffic will be allowed to pass (Stallings, p. 321, first #2 bullet point)," and that "[t]herefore, it is obvious to modify Reinert, as modified by Yadav, to include a firewall to protect the remote server from network-based security threats by installing a firewall to allow only authorized connections (i.e. the connections from the local computer), as taught by Stallings."

Appellant respectfully disagrees. Merely "modify[ing] Reinert, as modified by Yadav, to include a firewall to protect the remote server from network-based security threats by installing a firewall to allow only authorized connections," as suggested by the Examiner, does not even suggest that "network support code is used to **enable** said computer to establish said secure network connection via said firewall computer to said remote computer," especially where the network support code is loaded from removable physical media which specifically enables the secure network connection via the firewall, in the context claimed.

In addition, in the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "Reinert (and Reinert, as modified by Yadav) teaches a program (the claimed support code) establishing a network communication from the local computer to a remote server" and that "[t]herefore, Reinert discloses 'wherein said network support code is used to enable said computer to establish said secure network connection.'" The Examiner has further argued that "[t]he question raised is whether the support code (Reinert's communication program) would enable said computer to establish the connection via the firewall," and that "it is submitted that because network traffic is already produced by Reinert's communications program (the claimed support code), Reinert's communication program has the functionality to 'enable a connection to the remote computer via the firewall'". Additionally, the Examiner has argued that "[t]his is because the firewall alone decides what traffic is passed, not the communications program, and as described above, it is obvious for the firewall protecting the remote server to allow the traffic from Reinert's local computers to the remote server, as this is the traffic that is required to be authorized for Reinert's invention to work."

Appellant respectfully disagrees and asserts that simply "because network traffic is already produced by Reinert's communications program (the claimed support code)," as noted by the Examiner, does not inherently require "Reinert's communication program [to have] the functionality to 'enable a connection to the remote computer via the firewall'," as suggested by the Examiner. Reinert only discloses that the "communications program is invoked by the local user to establish a communications connection between the local computer 42 and the remote computer 54 via the communications hardware modems 40 and 58, respectively" (Col. 7, line 66-Col. 8, line 3), and not that "network support code is used to **enable** said computer to establish said secure network connection via said firewall computer to said remote computer," especially where the network support code is loaded from removable physical media which specifically enables the secure network connection via the firewall, in the context claimed.

It appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitation. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Additionally, in response, appellant asserts that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted

above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 29

With respect to Claim 29, the Examiner has relied on Col. 8, lines 14-16 and lines 25-31 from the Reinert reference to make a prior art showing of appellant's claimed technique "wherein said one or more malware detection files are determined based on said non-installed operating system."

Appellant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "a service program is downloaded from the remote computer 54 to the local computer 42" (Col. 8, lines 14-16 - emphasis added), and that "[d]ownloading the virus scanning software into the local computer memory 41 provides advantages ... because the virus scanning and virus repairing programs may be executed in the local computer memory" (Col.8, lines 25-29 – emphasis added). However, simply disclosing that a program is downloaded from the remote computer to the local computer and may be executed in local memory, as in Reinert, fails to even suggest that "one or more malware detection files are determined based on said non-installed operating system" (emphasis added), as specifically claimed by appellant.

In the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "the broad limitation 'based on' is not defined as such to require any specific connection or procedure tying the non-installed operation system with the malware detection files," and that "[i]t is submitted that since Reinert's non-installed operating system (Reinert's virus scanning program with communications program, Reinert col. 7, lines 62-67) retrieves the malware detection files (up-to-date virus signature file, col. 8, lines 20-25), the downloaded malware detection files are determined based on the virus scanning program and the communications program (non-installed operating system)." The Examiner has further argued that "[i]n the realm of Reinert's invention, the malware detection files would not be downloaded without the non-installed operating system and thus are determined 'based on the non-installed operating system.'"

Appellant respectfully disagrees. Reinert only discloses that the "communications program is invoked by the local user to establish a communications connection between the local computer 42 and the remote computer 54" (Col. 7, line 66-Col. 8, line 1), such that "the local user may then conduct...virus scanning" (Col. 8, lines 11-12), and that "[i]f the local computer 42 requests virus scanning services...a complete up-to-date virus signature file is downloaded into the local computer memory 41" (Col. 8, lines 20-25). However, merely invoking a communications program to establish a connection between the local computer and the remote computer such that a complete up-to-date virus signature file is downloaded into the local computer memory, as in Reinert, fails to specifically teach that "one or more malware detection files **are determined** based on said non-installed operating system" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 30

With respect to Claim 30, the Examiner has relied on Col. 8, lines 20-35 from the Reinert reference to make a prior art showing of appellant's claimed technique "wherein said one or more malware detection files are determined based on a malware detection product." Specifically, the Examiner has argued that "the virus detection signature file is used by the virus scanning software utility program."

Appellant respectfully disagrees and asserts that the excerpt relied upon by the Examiner merely teaches that "[i]f the local computer 42 requests virus scanning services, a virus scanning software utility program is downloaded into the local computer memory 41 via communications hardware modems 58 and 40, respectively," and that "a complete up-to-date virus signature file is downloaded into the local computer memory 41" (Col. 8, lines 20-25).

However, downloading a virus scanning software utility program as well as a virus signature file, as in Reinert, fails to specifically suggest a technique "wherein said one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by appellant. Moreover, asserting that "the virus detection signature file is used by the virus scanning software utility program," as argued by the Examiner, fails to suggest that "one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by appellant.

In the Examiner's Answer mailed 03/05/2008, the Examiner has argued that "it is submitted that since Reinert's malware detection product (Reinert's virus scanning program with communications program, Reinert col. 7, lines 62-67) retrieves the malware detection files (up-to-date virus signature file, col. 8, lines 20-25), the downloaded malware detection files are determined based on the virus scanning program and the communications program (Reinert's malware detection product)," and that "[i]n the realm of Reinert's invention, the malware detection files would not be downloaded without the malware detection product and thus are determined 'based on the malware detection product'".

Appellant respectfully disagrees. Reinert only discloses that the "communications program is invoked by the local user to establish a communications connection between the local computer 42 and the remote computer 54" (Col. 7, line 66-Col. 8, line 1), such that "the local user may then conduct...virus scanning" (Col. 8, lines 11-12), and that "[i]f the local computer 42 requests virus scanning services...a complete up-to-date virus signature file is downloaded into the local computer memory 41" (Col. 8, lines 20-25). However, merely invoking a communications program to establish a connection between the local computer and the remote computer such that a complete up-to-date virus signature file is downloaded into the local computer memory, as in Reinert, fails to specifically teach that "one or more malware detection files **are determined** based on a malware detection product" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted

above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue #2:

The Examiner has rejected Claims 26-27 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards), and in further view of Khatri (U.S. Patent No. 6,721,883).

Group #1: Claim 26

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Group #2: Claim 27

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Issue #3:

The Examiner has rejected Claim 31 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards"), and in further view of McCoskey (U.S. Publication No. 2003/0028889).

Group #1: Claim 31

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Issue #4:

The Examiner has not specifically rejected Claims 5, 9, 13, 17, 21, 25, and 31 under 35 U.S.C. 112. However, in the Office Action dated 05/15/2007, the Examiner has responded to appellant's arguments from the Amendment dated 03/12/2007 regarding the 35 U.S.C. 112 rejection from the Office Action dated 12/11/2006.

In the Examiner's Answer mailed 03/05/2008, the Examiner has stated that Issue #4 is not present for review and that there is no implied rejection under 35 U.S.C. 112.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NA11P492).

Respectfully submitted,

By: /KEVINZILKA/ Date: April 10, 2008
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660